

THAT WHICH IS CLAIMED IS:

1. A method for storing biometric information on a token comprising a magnetic storage medium, the method comprising:

capturing a biometric image and generating  
5 biometric data therefrom;  
generating a copy protect code; and  
storing the biometric data and the copy protect code on the magnetic storage medium of the token.

2. The method according to Claim 1, wherein the biometric information is based upon a fingerprint; and wherein capturing the biometric image comprises capturing the biometric image using a fingerprint  
5 sensor.

3. The method according to Claim 1, wherein the copy protect code is encrypted.

4. The method according to Claim 1, wherein wherein the token comprises a card corresponding to the ANSI/ISO/IEC 7810 standard and the magnetic storage medium comprises a magnetic stripe having  
5 three tracks in accordance with the ANSI/ISO/IEC 7810 standard; and wherein storing the biometric data and copy protect code comprises storing the biometric data and copy protect code on the third track of the magnetic stripe.

5. The method according to Claim 4, wherein

generating the copy protect code comprises combining at least some data stored on first and second tracks of the magnetic stripe.

5

6. The method according to Claim 1, wherein the array of image pixels comprises a series of consecutive and colinear image pixels.

7. The method according to Claim 1, wherein the token comprises a generally rectangular substrate.

8. The method according to Claim 1, wherein the token comprises at least one of an access card, credit card, debit card, identification card and smart card.

9. A method of regulating the use of a token, the token comprising a magnetic storage medium with biometric data and a copy protect code stored thereon, the method comprising:

5 capturing a biometric image and generating therefrom digital pixel data for an array of image pixels;

processing the digital pixel data to produce verification biometric data;

10 verifying the copy protect code stored on the magnetic medium; and

comparing the verification biometric data with the enrollment biometric data stored on the magnetic storage medium of the token to determine if  
15 the token holder is the authorized token user.

10. The method according to Claim 9, wherein the biometric information is based upon a fingerprint; and wherein capturing the biometric image comprises capturing the biometric image using a fingerprint sensor.

11. The method according to Claim 9, wherein the token comprises a card corresponding to the ANSI/ISO/IEC 7810 standard and the magnetic storage medium comprises a magnetic stripe having three tracks in accordance with the ANSI/ISO/IEC 7810 standard; and wherein the biometric data and copy protect code are stored on the third track of the magnetic stripe.

12. The method according to Claim 11, wherein verifying the copy protect code comprises:

reading the copy protect code stored on the third track of the magnetic stripe;

generating a verification copy protect code by calculating an LRC character based upon a combination of data stored on first and second tracks of the magnetic stripe; and

comparing the copy protect code read from the third track of the magnetic stripe with the verification copy protect code.

13. The method according to Claim 9, wherein the array of image pixels comprises a series of consecutive and colinear image pixels.

14. A method of regulating the use of a token,

the token comprising at least one of an access card, credit card, debit card, identification card and smart card, and including at least a magnetic storage

5 medium thereon, the method comprising:

enrolling an authorized token user by

capturing a first biometric image and  
generating therefrom first digital pixel data  
for a first array of image pixels,

10 processing the first digital pixel data to  
produce enrollment biometric data,

generating a copy protect code, and  
storing the enrollment biometric data and  
copy protect code on the magnetic storage medium

15 of the token; and

verifying an identity of a token holder

presenting the token by

capturing a second biometric image and  
generating therefrom second digital pixel data  
for a second array of image pixels,

20 processing the second digital pixel  
data to produce verification biometric data,

verifying the copy protect code stored on  
the magnetic medium, and

25 comparing the verification biometric data  
with the enrollment biometric data stored on the  
magnetic storage medium of the token to  
determine if the token holder is the authorized  
token user.

15. The method according to Claim 14, wherein  
the biometric information is based upon a  
fingerprint; and wherein capturing the biometric

images comprises capturing the biometric images using  
5 a fingerprint sensor.

16. The method according to Claim 14, wherein  
the copy protect code is encrypted.

17. The method according to Claim 14, wherein  
the token comprises a card corresponding to the  
ANSI/ISO/IEC 7810 standard and the magnetic storage  
medium comprises a magnetic stripe having three  
5 tracks in accordance with the ANSI/ISO/IEC 7810  
standard; and wherein storing the enrollment  
biometric data and copy protect code comprises  
storing the enrollment biometric data and copy  
protect code on the third track of the magnetic  
10 stripe.

18. The method according to Claim 17, wherein  
generating the copy protect code comprises  
calculating a longitudinal redundancy check (LRC)  
character based upon a combination of data stored on  
5 first and second tracks of the magnetic stripe.

19. The method according to Claim 18, wherein  
verifying the copy protect code comprises:  
reading the copy protect code stored on the third  
track of the magnetic stripe;  
5 generating a verification copy protect code by  
calculating a second LRC character based upon a  
combination of data stored on first and second tracks  
of the magnetic stripe; and  
comparing the copy protect code read from the

10 third track of the magnetic stripe with the  
verification copy protect code.

20. The method according to Claim 14, wherein  
the array of image pixels comprises a series of  
consecutive and colinear image pixels.

21. A system for regulating the use of a token,  
the token comprising at least one of an access card,  
credit card, debit card, identification card and  
smart card, and including at least a magnetic storage  
5 medium thereon, the system comprising:  
an authorized token user enrollment unit  
including  
a first biometric sensor device for  
capturing a first biometric image and generating  
therefrom first digital pixel data for a first  
10 array of image pixels,  
a first image processor for processing  
the first digital pixel data to produce  
enrollment biometric data,  
15 a copy protect code generator for  
generating a copy protect code, and  
a first magnetic storage medium  
reader/writer for writing the enrollment  
biometric data and the copy protect code on the  
20 magnetic storage medium of the token;  
at least one token holder verification unit for  
verifying the identity of a token holder presenting  
the token, and comprising  
a second biometric sensor device for  
25 capturing a second biometric image and

generating therefrom second digital pixel data  
for a second array of image pixels,

a second image processor for processing  
the second digital pixel data to produce  
30 verification biometric data,

a second magnetic storage medium  
reader for reading the enrollment  
biometric data and the copy protect code from  
the magnetic storage medium of the token,

35 a copy protect code verification unit for  
verifying the copy protect code, and

a comparator for comparing the verification  
biometric data produced by the second image  
processor with the enrollment biometric  
40 data stored on the magnetic storage medium of  
the token to determine if the token holder is  
the authorized token user.

22. The system according to Claim 21, wherein  
the biometric information is based upon a  
fingerprint; and wherein each of the biometric sensor  
devices comprises a fingerprint sensor.

23. The system according to Claim 22, wherein  
the biometric sensor device further comprises a  
finger slide adjacent the fingerprint sensor.

24. The system according to Claim 23, wherein  
the finger slide further comprises finger guides and  
a finger stop.

25. The system according to Claim 21, wherein

the copy protect code generator generates an encrypted copy protect code.

26. The system according to Claim 21, wherein the token comprises a card corresponding to the ANSI/ISO/IEC 7810 standard and the magnetic storage medium comprises a magnetic stripe having three  
5 tracks in accordance with the ANSI/ISO/IEC 7810 standard; and wherein the first magnetic storage medium reader/writer writes the enrollment biometric data and copy protect code on the third track of the magnetic stripe.

27. The system according to Claim 21, wherein the copy protect code generator comprises a longitudinal redundancy check (LRC) character calculator for calculating an LRC character based  
5 upon a combination of data stored on first and second tracks of the magnetic stripe.

28. The system according to Claim 27, wherein the copy protect code verification unit comprises: a second LRC calculator for calculating a second LRC character based upon a combination of data stored on  
5 first and second tracks of the magnetic stripe to generate a verification copy protect code; and a code comparator for comparing the copy protect code stored on the third track of the magnetic stripe with the verification copy protect code.

29. The system according to Claim 21, wherein the array of image pixels comprises a series of



consecutive and colinear image pixels.

20230101 000000